UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/992,582	11/16/2001	Stephen M. Hitchen	7216-1	8250

7590 04/30/2004

Steven M. Greenberg
Akerman, Senterfitt & Eidson, P.A.
Post Office Box 3188
West Palm Beach, FL 33402-3188

EXAMINER	
WASSUM, LUKE S	

ART UNIT	PAPER NUMBER
2177	5

DATE MAILED: 04/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/992,582	HITCHEN ET AL.	
	Examiner	Art Unit	
	Luke S. Wassum	2177	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2 and 4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The Applicants' Information Disclosure Statements, filed 16 November 2001 and 13 May 2002, have been received and entered into the record. Since the Information Disclosure Statements comply with the provisions of MPEP § 609, the references cited therein have been considered by the examiner. See attached forms PTO-1449.

The Invention

2. The claimed invention is a collaborative rights management system for distributing documents with digital rights management data appended, thus preserving the integrity of the documents by enforcing specific digital rights on a user-by-user basis.

Claim Objections

3. Claims 3 and 15 are objected to because of the following informalities:

In both cases, the claim does not end with a period.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* v. *John Deere Co*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Morinaga et al.** (U.S. Patent 5,724,578) in view of **McCurdy et al.** (U.S. Patent Application Publication 2002/0035697).

8. Regarding claim **1, Morinaga et al.** teaches a collaborative file rights management method as claimed, comprising:

a) identifying a file input/output (I/O) request to access a file, said file I/O request originating in an authoring application (see col. 4, lines 20-23, disclosing that all requests for files are received by the file transaction control unit);

b) suppressing said file I/O request (see col. 4, lines 24-28, disclosing that file operation control unit);

c) automatically extracting digital rights management data appended to said file (see disclosure of the file control block, col. 4, lines 32-61); and

d) providing said file to said authoring application (see col. 4, lines 32-38; see also col. 7, lines 35-46).

Morinaga et al. does not explicitly teach a collaborative file rights management method including the step of managing access to said file in said authoring application based upon said extracted digital rights management data.

McCurdy et al., however, teaches a collaborative file rights management method including managing access to said file in said authoring application based upon said extracted digital rights management data (see paragraphs [0137] through [0140]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform the claimed intercepting, detecting and quashing steps in cooperation with an authoring application, since digital rights management dictates that users with no rights to individual parts of a document be prohibited from copying not only an entire document, but the individual protected parts (see paragraphs [0137] and [0138]).

9. Regarding claim 9, **Morinaga et al.** teaches a collaborative file rights management method as claimed, comprising:

a) identifying a file input/output (I/O) request to save a file, said file I/O request originating in an authoring application (see col. 4, lines 20-23, disclosing that all requests for files are received by the file transaction control unit);

b) suppressing said file I/O request (see col. 4, lines 24-28, disclosing that file operation control unit);

c) appending digital rights management to said file (see disclosure of the file control block, col. 4, lines 32-61); and

d) storing said file in fixed storage (see col. 4, lines 44-61; see also col. 7, lines 61-65).

Morinaga et al. does not explicitly teach a collaborative file rights management method including the step of automatically encrypting the file.

McCurdy et al., however, teaches a collaborative file rights management method including the step of automatically encrypting the file (see paragraph [0016]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to automatically encrypt a saved file, since encryption is a well known and widely used technique for protecting data and/or files from access by unauthorized users.

10. Regarding claim 12, **Morinaga et al.** teaches a collaborative file rights management system as claimed, comprising:

a) a file security management application configured to intercept operating system messages directed to an authoring application (see col. 4, lines 20-23, disclosing that all requests for files are received by the file transaction control unit);

b) a file security filter driver configured to identify file input/output (I/O) requests received in a kernel-layer system manager to open a file in said authoring application (see col. 4, lines 32-38; see also col. 7, lines 35-46);

c) said file security driver quashing said file I/O requests and providing said file to said authoring application (see col. 4, lines 32-38; see also col. 7, lines 35-46);

d) said file security management application extracting digital rights management data appended to said file, detecting among intercepted operating system messages operating system messages directed to authoring applications which can be limited according to digital rights specified in said extracted digital rights management data and quashing said detected events where said digital rights management data prohibits execution of said authoring application operations (see disclosure of the file control block, col. 4, lines 32-61; see also col. 8, lines 10-16).

Morinaga et al. does not explicitly teach a collaborative file rights management system including the automatic encryption and decryption of the file.

McCurdy et al., however, teaches a collaborative file rights management method further comprising automatically encrypting said file (see paragraph [0016]) and decrypting said file (see paragraph [0205].

It would have been obvious to one of ordinary skill in the art at the time of the invention to automatically decrypt a retrieved file, since encryption/decryption is a well known and widely used technique for protecting data and/or files from access by unauthorized users, and decryption is necessary for an authorized user to access an encrypted file.

11. Regarding claim 13, **Morinaga et al.** teaches a machine readable storage having stored thereon a computer program for managing digital rights in a collaborative file, said computer program comprising a routine set of instructions for causing the machine to perform the steps of:

a) identifying a file input/output (I/O) request to access a file, said file I/O request originating in an authoring application (see col. 4, lines 20-23, disclosing that all requests for files are received by the file transaction control unit);

b) suppressing said file I/O request (see col. 4, lines 24-28, disclosing that file operation control unit);

c) automatically extracting digital rights management data appended to said file (see disclosure of the file control block, col. 4, lines 32-61); and

d) providing said file to said authoring application (see col. 4, lines 32-38; see also col. 7, lines 35-46).

Morinaga et al. does not explicitly teach a computer program for managing digital rights including the step of managing access to said file in said authoring application based upon said extracted digital rights management data.

McCurdy et al., however, teaches a computer program for managing digital rights including managing access to said file in said authoring application based upon said extracted digital rights management data (see paragraphs [0137] through [0140]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform the claimed intercepting, detecting and quashing steps in cooperation with an authoring application, since digital rights management dictates that users with no rights to individual parts of a document be prohibited from copying not only an entire document, but the individual protected parts (see paragraphs [0137] and [0138]).

12. Regarding claims 2 and 14, **McCurdy et al.**, however, teaches a collaborative file rights management method and computer program for managing digital rights further comprising decrypting said file (see paragraph [0205].

It would have been obvious to one of ordinary skill in the art at the time of the invention to automatically decrypt a retrieved file, since encryption/decryption is a well known and widely used

technique for protecting data and/or files from access by unauthorized users, and decryption is necessary for an authorized user to access an encrypted file.

13. Regarding claims 3 and 15, **Morinaga et al.** additionally teaches a collaborative file rights management method and computer program for managing digital rights wherein said extracting step further comprises:

a) determining environmental data associated with said I/O request, said environmental data comprising at least one of a requestor's identity, a requestor's class, a requestor's computing domain, a requestor's location, a password, a time of day, and a date (see registration of the requestor's identity, col. 7, lines 16-21; see also col. 7, lines 35-46); and

extracting an access policy appended to said file (see file control block in Figure 3A, including access rights based upon the specific requestor's identity).

14. Regarding claims 4 and 16, **Morinaga et al.** additionally teaches a collaborative file rights management method and computer program for managing digital rights wherein said providing step further comprises:

a) comparing said access policy to at least a portion of said environmental data (see col. 4, lines 32-62; see also col. 7, lines 35-46);

b) authenticating said file I/O request based upon said comparison (see col. 4, lines 32-62; see also col. 7, lines 35-46); and

c) providing said file to said authoring application only if said I/O request has been authenticated (see col. 4, lines 32-62; see also col. 7, lines 35-46).

15. Regarding claims 5, 10 and 17, **Morinaga et al.** additionally teaches a collaborative file rights management method and computer program for managing digital rights wherein said suppressing step further comprises:

a) posting a responsive message to said authoring application (see col. 8, lines 10-16);

b) intercepting an operating system event in said authoring application, said operating system event indicating receipt of said responsive message (see col. 8, lines 10-16); and

c) quashing further processing of said intercepted operating system event (see col. 8, lines 10-16).

16. Regarding claims 6, 11 and 18, **Morinaga et al.** additionally teaches a collaborative file rights management method and computer program for managing digital rights wherein said identifying step comprises:

a) monitoring kernel-level file I/O requests contained in I/O request packets processed in a file system manager (see col. 4, lines 20-28); and

b) detecting said file I/O request to access said file in one of said I/O request packets (see col. 4, lines 20-28).

17. Regarding claims 7, 8, 19 and 20, **Morinaga et al.** teaches a collaborative file rights management method and computer program for managing digital rights substantially as claimed.

Morinaga et al. does not explicitly teach a collaborative file rights management method and computer program for managing digital rights wherein said management step comprises the claimed

intercepting, detecting and quashing steps in cooperation with an authoring application wherein the protected operations are selected from clipboard operations, printing operations, file saving operations and file editing operations.

McCurdy et al., however, teaches a collaborative file rights management method and computer program for managing digital rights wherein said management step comprises:

a) intercepting operating system messages in said authoring application (see paragraphs [0137] through [0140]);

b) detecting among said intercepted operating system messages, operating system messages directed to authoring application operations which can be limited according to digital rights specified in said extracted digital rights management data, wherein the protected operations are selected from clipboard operations, printing operations, file saving operations and file editing operations (see paragraphs [0137] through [0140]); and

c) quashing said detected events where said digital rights management data prohibits execution of said authoring application operations (see paragraphs [0137] through [0140]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform the claimed intercepting, detecting and quashing steps in cooperation with an authoring application, since digital rights management dictates that users with no rights to individual parts of a document be prohibited from copying not only an entire document, but the individual protected parts (see paragraphs [0137] and [0138]).

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Moir (U.S. Patent 5,113,442) teaches a method for controlling access rights among a plurality of users to a plurality of secure objects.

Kohari (U.S. Patent 5,291,405) teaches a document management system suitable for managing preparation, routing and approval of documents, such as routine approval slips and communication sheets, in which reading and writing are generally restricted to particular persons.

Nishiyama (U.S. Patent 5,778,365) teaches a file management device for managing a file accessed by a plurality of users which comprises setting means for setting a plurality of attribute values related to a particular attribute of the file, and for setting access rights in accordance with the plurality of attribute values related to the attribute.

McDonnal et al. (U.S. Patent 5,796,825) teaches a system for automatic decryption of file data on a per-user basis and automatic re-encryption.

Hsieh (U.S. Patent 5,925,126) teaches a security shield implementation method that intercepts system calls to control access by a user of the computer system software.

Golan (U.S. Patent 5,974,549) teaches a method of creating a secure sandbox within a plurality of downloaded software components that can execute in a secure manner.

Glover (U.S. Patent 6,052,780) teaches a computer system for accessing an encrypted and self-decrypting digital information product while restricting access to decrypted digital information.

Zizzi (U.S. Patent 6,185,681) teaches a method of transparent encryption and decryption for an electronic document management system.

Dourish et al. (U.S. Patent 6,253,217) teaches a document management system which organizes, stores and retrieves documents according to properties attached to the documents.

Pensak et al. (U.S. Patent 6,289,450) teaches an information security architecture for encrypting documents for remote access while maintaining access control.

Petersen et al. (U.S. Patent 6,308,179) teaches a user-level controlled mechanism for attaching properties to documents.

Starek et al. (U.S. Patent 6,314,437) teaches a method for enhancing file system calls to provide real-time secure file deletion on an ongoing basis.

Lamping et al. (U.S. Patent 6,324,551) teaches a document management system which organizes, stores and retrieves documents according to properties attached to the documents.

Pensak et al. (U.S. Patent 6,339,825) teaches an information security architecture for encrypting documents for remote access while maintaining access control.

Blumenau et al. (U.S. Patent 6,449,652) teaches a method for managing access to one of a plurality of raw storage devices that stores data accessed by a host computer.

Pensak et al. (U.S. Patent 6,449,721) teaches an information security architecture for encrypting documents for remote access while maintaining access control.

Friedman et al. (U.S. Patent 6,553,466) teaches a shared memory blocking method in which protected data is transmitted to a recipient computer.

O'Brien et al. (U.S. Patent 6,658,571) teaches a security framework for wrapping standard, commercially available software applications in order to limit the amount of potential damage that a successful attacker or corrupt program can cause.

Brown et al. (U.S. Patent 6,671,805) teaches a method for digitally signing an electronic document by a plurality of signers, including determining a signing role for each signer.

Friedman et al. (International Publication WO 01/25925) teaches a port blocking method in which protected data is segregated from other data, which allows ports to be opened only by processes which do not have access to secured data.

Friedman et al. (International Publication WO 01/25928) teaches a clock monitoring system having a memory for storing a permission database having one or more permission fields, each field comprising one or more clock-related permissions and a time-value field comprising a stored time-value to prevent unauthorized access on a computer.

Friedman et al. (International Publication WO 01/25932) teaches a file system security driver and vault system in which protected data is segregated form other data, which allows for back-channeling of file data to ensure that files created by applications using secured data do not cause leaks of secure data.

Friedman et al. (International Publication WO 01/25937) teaches a network blocking method in which protected data is segregated from other data, which allows a network connection to be opened only by processes which do not have access to secured data.

Friedman et al. (International Publication WO 01/25953) teaches a registry monitoring method applicable to a system in which protected data is segregated form other data, in which protected data is transmitted to a recipient computer.

Friedman et al. (International Publication WO 01/26276) teaches a system for providing data security in a device driver.

Friedman et al. (International Publication WO 01/26277) teaches a system for communicating a package of information.

Dourish et al. ("Extending Document Managemtn Systems with User-Specific Active Properties") teaches a prototype system developed to explore a property-based document

management system with active properties that carry executable code to enable document-based services on a property infrastructure.

Infraworks Corporation ("Solutions for File Protection") teaches the InTether system, which addresses file protection issues facing today's corporate users.

DeMarines ("Content Security for the Enterprise") teaches a comprehensive content security solution that can be easily deployed and integrated with existing infrastructure.

The following references, while not qualifying as prior art, are also of interest:

Brew et al. (U.S. Patent Application Publication 2003/0196114) teaches a system for providing persistent access control pf protected content.

Seeman (U.S. Patent Application Publication 2003/0200459) teaches a computer data security system including a file decrypter for decrypting encoded files and an encrypter for re-encrypting decrypted files that have been modified.

Bar-Or et al. (U.S. Patent Application Publication 2003/0237005) teaches a method of protecting digital objects distributed over a network by electronic mail.

Dourish ("The Appropriation of Interactive Technologies: Some Lessons from Placeless Documents") teaches recent appropriation of technical features supporting collaborative systems.

DeMarines ("IP on the Move: Protecting Intellectual Property in a Competitive Manufacturing Environment") teaches issues and solutions in sharing sensitive intellectual property such as product specifications and price books with outside partners.

Infraworks Corporation ("InTether™ Server") is a product brochure.

Infraworks Corporation ("InTether™ Desktop") is a product brochure.

Adhaero Technologies ("Adhaero Doc Technical Overview") provides an overview of the features of the Adhaero Doc product.

Adhaero Technologies ("Business Document Security with Adhaero Doc") teaches applications of the Adhaero Doc product.

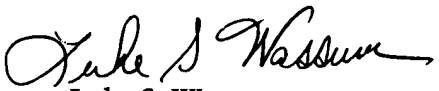
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luke S. Wassum whose telephone number is 703-305-5706. The examiner can normally be reached on Monday-Friday 8:30-5:30, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on 703-305-9790. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

In addition, INFORMAL or DRAFT communications may be faxed directly to the examiner at 703-746-5658.

Customer Service for Tech Center 2100 can be reached during regular business hours at (703) 306-5631, or fax (703) 746-7240.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Luke S. Wassum
Art Unit 2177

lsw
27 April 2004